The International Center for Not-for-Profit Law
1126 16th Street NW, Suite 400
Washington, DC 20036
Contact: Zach Lampell, Legal Advisor
zlampell@icnl.org

INTRODUCTION

On April 16, 2015, Pakistan's National Assembly Standing Committee on Information Technology and Telecommunication approved a draft of the Prevention of Electronic Crimes Bill, 2015 (PECA). The Chairman of National Assembly Standing Committee on Information Technology has made the latest draft available to the public and invited the general public and other stakeholders to submit written objections on the relevant clauses of the PECA.[1] The PECA now awaits consideration by the National Assembly and Senate.

The Government of Pakistan has stated that the PECA is intended to protect the freedom of expression. While ICNL applauds the Pakistani government for aiming to protect the freedom of expression, for making the PECA available to the public and for seeking public consultation and comments, ICNL is concerned that the PECA, in its current form, contains provisions that violate international standards of the freedom of expression and the right to privacy. Key concerns include the following:

- Data Retention and Intermediary Liability – the PECA requires any internet provider, which includes anyone that provides a premise or facility for the public to access the internet, to store internet data for at least 1 year and produce it when ordered by authorities, regardless of whether such production is lawful;

- Duplicative Crimes – the PECA recriminalizes actions already criminalized in Pakistan's Penal code, which may result in similar conduct being treated differently and inconsistently;

- Vague Language Affecting the Freedom of Expression – the PECA contains vague language that may invite arbitrary and subjective application, resulting in violations of the freedom of expression and Pakistan's obligations under the ICCPR;

[1] The Prevention of Electronic Crimes Bill, 2015 (PECA) is available on the websites of the National Assembly (www.na.gov.pk) and Ministry of IT (www.moit.gov.pk); ICNL retrieved the PECA from: http://www.moit.gov.pk/gop/index.php?q=aHR0cDovLzE5Mi4xNjguNzAuMTM2L21vaXQvdXNlcmZpbGVzMS9maWxlL0RyYWZ0JTIwUEVDJTIwQmlsbCUyMDIyJTIwQXByaWwlMjAxNS5wZGY%3D (last accessed: May 4, 2015).

- Vague Language Affecting the Right to Privacy – the PECA contains vague language that may invite arbitrary and subjective application, resulting in violations to the right to privacy and Pakistan's obligations under the ICCPR; and

- Expansive Investigatory Powers – the PECA creates a new investigatory agency and provides that agency with expansive, over-reaching surveillance powers with little, if any, meaningful judicial oversight, which will likely curtail the exercise of the freedom of expression and the right to privacy.

RELEVANT INTERNATIONAL LAW

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) requires State parties to guarantee the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers.[2] The full text of Article 19 reads:

> 1. Everyone shall have the right to hold opinions without interference.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

The Human Rights Committee has stated that, "any restrictions on the operation of websites, blogs, or any other internet-based electron or other such information dissemination systems" must comply with Article 19.[3] Restrictions to the speech and expressions guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test:

> (1) the restriction must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
> (2) the restriction must pursue one of the purposes set out in article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and
> (3) the restriction must be proven as necessary and the least restrictive

[2] Pakistan ratified the ICCPR in 2010.

[3] Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 43, UN Doc # CCPR/C/GC/34 (2011).

> means required to achieve the purported aim (principles of necessity and proportionality).[4]

Similarly, the right to privacy is enshrined in Article 17 of the ICCPR, "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from State intervention.[5] "In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous."[6]

Although Article 17 envisages necessary, legitimate and proportionate restrictions to the right to privacy, the Special Rapporteur for Freedom of Expression (Special Rapporteur) states that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, elucidated in the Human Rights Committee General Comment 27, paragraph 15:

> (a) Any restrictions must be provided by the law;
> (b) The essence of a human right is not subject to restrictions;
> (c) Restrictions must be necessary in a democratic society;
> (d) Any discretion exercised when implementing the restrictions must not be unfettered;
> (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim; and
> (f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected.[7]

The freedom of expression and the right to privacy are interrelated, "the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression."[8] Limitations or restrictions to one of these rights impact the enjoyment of the other. Just as a

---

[4] See, e.g. Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 69, UN Doc. # A/HRC/17/27 (May 2011).

[5] See, Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, Butterworth, 2004, para. 4.82

[6] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 23, UN Doc. # A/HRC/23/40 (April 2013).

[7] Human Rights Committee, General Comment No. 27: Freedom of Movement (Article 12), para. 15, UN Doc # CCPR/C/21/Rev.1/Add.9 (1999); Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 29, UN Doc. # A/HRC/23/40 (April 2013).

[8] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 24, UN Doc. # A/HRC/23/40 (April 2013).

restriction to the freedom of expression must pass the three-part cumulative test derived from ICCPR Article 19 to be lawful, a restriction to the right to privacy is only lawful if it passes the test articulated in General Comment 27.15.[9]

ANALYSIS

The articles highlighted below fail the respective tests rooted in the ICCPR for being either too vague or not adhering to the principles of necessity and proportionality. The goal of these comments is to highlight problematic provisions, briefly address why they may be found to restrict the freedom of expression or right to privacy, and, where appropriate, offer suggestions on how to revise the language of the PECA.

As a threshold issue, we note the fact that the PECA adopts broad definitions of certain key words. The term "intelligence" is defined as "any speech, sound, data, signal, writing, image or video."[10] "Intelligence" includes any and all types of electronic communications, which is different from its ordinary meaning. Similarly, the term "device" is defined as including, "any electronic or virtual tool that is not in physical form," and "a password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed."[11] These terms include a broad range of items that are not traditionally considered "intelligence" or a "device." While States are free to define terms in legislation, care should be taken to use generally accepted definitions as much as possible because this allows laws to be easily understood.

1. Data Retention and Intermediary Liability

Article 29 requires service providers – broadly defined to include not only traditional telecommunications providers, but also anyone that provides a premise or facility for the public to access the Internet, i.e. café owners[12] – to retain all "traffic data" for a period of at least 1 year

[9] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 29, UN Doc. # A/HRC/23/40 (April 2013).

[10] PECA, Article 2(t).

[11] PECA, Article 2(o)ii and iii.

[12] PECA, Article 2(aa): "'service provider' includes a person who: (i) acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system; (ii) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; (iii) processes or stores data on behalf of such electronic communication service or users of such service; or (iv) provides premises from where or facilities through which the public in general may access an information system and the internet such as cyber cafes;"

or as directed by the Pakistan Telecommunication Authority (Authority).[13] Additionally, every service provider must provide that data to the investigation agency or authorised officer "whenever so required." Owners of cafes, bookstores, restaurants or any other place offering internet access to the public are subject to this requirement. This compulsory data retention is concerning on a number of levels as it directly threatens the freedoms of expression and privacy.

Bulk compulsory data retention increases the scope of State surveillance, increases business expenses, which lowers profits, and increases the likelihood that the data will be stolen, accidentally disclosed or used to commit fraud.[14] The definition of "service provider" is so broad that many small business owners are considered "service providers," even though they likely do not have the knowledge or expertise to retain the potentially vast amounts of data. The Authority has the power to order data retention indefinitely, which will only further increase the burden of "service providers" to comply with the PECA. There is no judicial oversight over these orders, which potentially places "service providers" in a difficult situation; either they comply with the orders even if those orders are illegal or unconstitutional and then risk being punished for acting illegally, or they refuse to comply with the orders and are prosecuted under the PECA.[15]

Recommendation: Article 29 should be revised to address these concerns; in particular the term "service provider" should be re-defined, the bulk data retention requirement should be deleted and service providers should be not liable for refusing to produce data.

2. Duplicative Crimes

To the greatest extent possible electronic crimes laws, or Cybercrime laws, should focus on actions genuinely and directly related to computer information and systems. By recriminalizing actions, the PECA creates the risk that similar conduct may be treated differently and inconsistently, depending on which law is applied. The articles noted in this section should be deleted from the PECA and, if necessary, the Penal Code should be amended to cover specific computer-related actions to ensure that the traditional offence can be applied in an electronic environment.

Article 11 – Electronic forgery

This article prohibits electronic forgery.[16] Although this article is well defined it duplicates provisions in the Penal Code, specifically articles 415 and 416.

[13] PECA, Article 29(1): "A service provider shall, within its existing or required technical capability, retain its traffic data for a minimum period of one year or such period as the Authority may notify from time to time and provide that data to the investigation agency or the authorised officer whenever so required."

[14] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 67, UN Doc. # A/HRC/23/40, (April 2013).

[15] PECA, Article 29(3): "Any person who contravenes the provisions of this section [Article 29] shall be punished with imprisonment for a term which may extend to six months or with a fine up to five hundred thousand rupees or both."

[16] PECA, Article 11(1): "Whoever, intentionally interferes with or uses any information system, device or data, to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input,

Recommendation: Article 11 should be deleted since the actions covered are already addressed in the Penal Code. Should the Penal Code be found not to cover electronic forgery, the Penal Code should be amended.

Article 12 – Electronic fraud

Article 12 prohibits electronic fraud, but is problematic since it does not require any real or tangible damage or harm to occur – the standard articulated in Article 12 is "likely to cause damage or harm."[17]

Recommendation: Article 12 should either be deleted or amended. The actions covered in Article 12 are already covered in the Penal Code, specifically Articles 415, 416 and 425, and therefore it is unnecessary to include these issues in the PECA. Should the Penal Code be found not to address electronic fraud, the Penal Code should be amended. If the actions described in Article 12 cannot be included into the Penal Code, then Article 12 should be rewritten to require that specific harm or damages occur before electronic fraud is committed.

Article 18 – Offenses against dignity of natural persons

Article 18 is essentially a criminal defamation provision designed to cover any and all "intelligence."[18] Defamation is already included in the Penal Code, Article 499, and likely covers all of actions described in Article 18.

Criminal defamation laws impermissibly restrict the freedom of expression. In General Comment no. 34, the UN Human Rights Committee recommended that States consider decriminalizing defamation and that criminal penalties should only be applied in the most serious cases.[19] Additionally, the Special Rapporteur has repeatedly and consistently called for a prohibition of

---

alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not shall be punished with imprisonment of either description for a term which may extend to three years, or with fine up to two hundred and fifty thousand rupees or with both."

[17] PECA, Article 12: "Whoever intentionally, for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extent to two years or with fine up to ten million rupees, or with both."

[18] PECA, Article 18: "(1) Whoever intentionally publicly exhibits or displays or transmits any false intelligence, which is likely to harm or intimidate the reputation or privacy of a natural person shall be punished with imprisonment for a term which may extend to three years or with fine up to one million rupees or with both: Provided, nothing under this sub-section (1) shall apply to anything aired by a broadcast media or distribution service licensed under Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).
(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for passing of such orders for removal, destruction or blocking access to such intelligence referred to in sub- section (1) and the Authority on receipt of such application, may take such measures as deemed appropriate for securing, destroying, blocking access or preventing transmission of such intelligence."

[19] Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 47, UN Doc # CCPR/C/GC/34 (2011).

criminal defamation because, "criminalization can be counter-effective and the threat of harsh sanctions exert a significant chilling effect on the right to freedom of expression."[20]

In addition to criminal penalties, Article 18 permits the Authority to destroy, remove and/or block such offending intelligence. This impermissibly restricts the freedom of expression,[21] and there is no independent or judicial oversight as to the removal, destruction or blocking of such content.

Recommendation: Article 18 should be deleted from the PECA, as it is duplicative. Moreover, criminal defamation is an impermissible restriction on the freedom of expression *per se* and Article 18 should be deleted on that ground, as well.

3. Vague Language Affecting the Freedom of Expression

The following articles likely impose unlawful restrictions to the freedom of expression due to vague language used in the PECA. The use of vague language can open the door to arbitrary interpretation and enforcement. ICNL is concerned by the use of vague language in the following provisions.

Article 9 – Glorification of an offence and hate speech

Article 9 prohibits glorifying an offence or a person accused of a crime, supporting terrorism or activities of a terrorist organization, and advancing religious, ethnic or sectarian hatred.[22] This offense is overly broad and likely constitutes an impermissible restriction on the freedom of expression.

[20] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 40, UN Doc. # A/66/290 (August 2011).

[21] See, Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 31, UN Doc. # A/HRC/17/27 (May 2011), "Firstly, the specific conditions that justify blocking are not established in law, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body."

[22] PECA, Article 9: "Whoever prepares or disseminates intelligence, through any information system or device, where the commission or threat is with the intent to: (a) glorify an offence or the person accused or convicted of a crime; (b) support terrorism or activities of proscribed organizations; and (c) advance religious, ethnic or sectarian hatred shall be punished with imprisonment for a term which may extend to five years or with fine up to ten million rupees or with both.

First, criminalizing the "glorification"[23] of an offence or a person accused or convicted of a crime will likely prevent meaningful debate about whether an individual was rightfully accused or convicted of a crime. This provision criminalizes the "glorification" of a person merely accused of a crime, which could impact reporting on human rights and human rights defenders. Supporters of an individual accused of a crime could be jailed for merely expressing their support of that individual, who upon trial may be acquitted of the crime for which he/she was charged. This would amount to an unlawful restriction on speech.[24]

Second, the term "support" of terrorism is vague and unclear. The Special Rapporteur has stated that the use of term "glorification" of terrorism is too vague to meet the requirements of the three-part test from Article 19 of the ICCPR.[25]

Recommendation: Article 9 should be removed. The Government of Pakistan, if its goal is to prohibit incitement to discrimination, hostility or violence or incitement to terrorism, should replace Article 9 with a provision that narrowly and specifically prohibits incitement to discrimination, hostility, violence or terrorism.

Article 10 – Cyber Terrorism

Article 10 prohibits Cyber terrorism,[26] including threats to commit offenses outlined in Articles 6-9 of the PECA. This provision is overly broad and vague, and should be linked to actual violence, specifically harming individuals. A social media user could be imprisoned under this article if he publishes a post supporting a political party since that may create "insecurity in the Government." This article is further problematic because anyone accused under it cannot be granted bail,[27] which may violate the right to liberty and freedom from arbitrary arrest and detention.[28]

Recommendation: This article should be deleted as it impermissibly restricts speech. Additionally, the issues covered in Article 10 are already addressed and criminalized in the Protection of Pakistan Act and Pakistan's Penal Code.

---

[23] The PECA explains "Glorification" as "include[ing] depiction of any form of praise or celebration in a desirable manner."

[24] Human Rights Council, *Resolution: Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*, para. 5, UN Doc # A/HRC/RES/12/16 (October 12, 2009).

[25] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 34, UN Doc. # A/66/290 (August 2011).

[26] PECA, Article 10: Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9 of this Act, where the commission or threat is with the intent to: (a) coerce, intimidate, overawe or create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance religious, ethnic or sectarian discord, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine up to fifty million rupees or with both.

[27] PECA, Article 38(2).

[28] See ICCPR, Article 9.

Article 19 – Offenses against modesty of a natural person and minor

This article prohibits the publication or transmission of "any intelligence which (a) superimposes a photograph of the face of a natural person over any sexually explicit image; or (b) distorts the face of a natural person or the inclusion of a photograph or a video of a natural person in a sexually explicit conduct; or (c) intimidates a natural person with any sexual act." As written, this article is overly broad and vague, requires no showing of harm, and is likely to stifle and/or suppress humor. Because the words in Article 19 are susceptible to subjective and possibly distorted interpretations, there is real concern that this article could be used to stifle unpopular speech. In sum, this article amounts to an impermissible restriction of the freedom of expression, as it cannot pass the cumulative test set forth in Article 19 of the ICCPR.

This Article is further problematic because anyone accused under it cannot be granted bail,[29] which may violate the right to liberty and freedom from arbitrary arrest and detention.[30]

Recommendation: Article 19 should be removed.

Article 21 – Cyber stalking

The crime of "cyber stalking" prohibits using electronic means of communication to: "(a) communicate obscene, vulgar, contemptuous, or indecent intelligence; or (b) to make any suggestion or proposal of an obscene nature; or (c) threaten to commit any illegal or immoral act; or (d) take a picture or photograph of any person and display or distribute without his concern or consent or knowledge in a manner that harms the person; or (e) display or distribute information in a manner that substantially increases the risk of harm or violence to any person," when there is an intent to coerce, intimidate or harass the subject of the communication. The prohibition of communicating "obscene, vulgar, contemptuous or indecent intelligence," is overly broad and vague, as the terms themselves are undefined and subject to interpretation. In addition to journalists being subject to arrest for merely taking and publishing photographs of news events, ordinary citizens may be prosecuted under Article 21 for insulting or mocking anyone else.

Taken as whole, this article likely does not comply with Article 19 of the ICCPR as it unlawfully restricts the freedom of expression.

Recommendation: Article 21 should be deleted or substantially rewritten with narrow, concise, well-defined language in order to meet the requirements of ICCPR Article 19.

Article 23 - Spoofing

This article defines a new crime – spoofing – which prohibits the establishment of a website or the sending of intelligence with a counterfeit source "intended to be believed by the recipient or visitor of the website, to be an authentic source…" This article may jeopardize parody websites, which would thus restrict the freedom of expression.

[29] PECA, Article 38(2).

[30] See ICCPR, Article 9.

Recommendation: This article should be revised to strengthen the intent element and to carve out exceptions for websites that are meant to be humorous, parodies or artistic.

4. Vague Language Affecting the Right to Privacy

The following articles likely impose unlawful limitations to the right to privacy due to vague language used in the PECA. These articles should be revised to comply with international human rights law or should be deleted from the PECA.

Article 15 – Unauthorised issuance of SIM cards etc.
This article prohibits the unauthorised selling, issuance or providing of SIM cards or R-IUM chips or usage in cellular mobile or wireless phones.[31] It is unclear from the language used in Article 15 if legitimate conduct, such as lending a SIM card to a family member or friend, is criminalized. ICNL reiterates the concern expressed by the Special Rapporteur that requiring all mobile phone users to register with government authorities without data protection legislation amounts to a restriction on the right to privacy in one's communications.[32]

Recommendation: Article 15 should be deleted until such time as data protection legislation is adopted, and at that point Article 15 should be revised with clearer language so that legitimate conduct cannot be considered illegal.

Article 16
This article prohibits changes to the "unique device identifier" of any mobile wireless communication device.[33] Article 16 is worded so broadly that such prohibition may extend to encryption devices or software. ICNL reiterates the concern of the Special Rapporteur that limitations of the use of privacy-enhancing tools that can be used to protect communications amounts to a restriction on the right to privacy in one's communications.[34]

[31] PECA, Article 15: "Whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for transmitting intelligence without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine up to five hundred thousand rupees or both."

[32] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 70, UN Doc. # A/HRC/23/40, (April 2013).

[33] PECA, Article 16: "Whoever unlawfully or without authorisation changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving intelligence shall be punished with imprisonment which may extend to three years or with fine up to one million rupees or both. Explanation: A 'unique device identifier' is an electronic equipment identifier which is unique to a mobile wireless communication device."

[34] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 71, UN Doc. # A/HRC/23/40, (April 2013).

Recommendation: This Article should be amended to specifically permit the use of privacy-enhancing tools, including encryption devices and software.

5. Expansive Investigatory Powers

Chapter III establishes a new investigatory agency tasked with investigating alleged crimes under the PECA and outlines the procedural powers of this new agency and its officers. The articles in Chapter III are all interrelated, with powers bestowed in one article enhanced, clarified or constrained in the next. When Chapter III is reviewed in its entirety, it is clear that the new investigatory agency will have vast surveillance powers with little to no meaningful judicial oversight, which will greatly affect the freedom of expression and right to privacy inside and outside Pakistan.[35] The powers proscribed to the investigatory agency and its officers need to be reigned in to prevent the possibility of abuse. Chapter III is reviewed below as a series of connected articles and powers.

Article 26 permits the Government of Pakistan to establish or designate a law enforcement agency as the "investigative agency" to look into offenses under the PECA.[36] Article 26, however, does not explain which agency or agencies would regulate this investigative agency. Without a clear delineation of authority, the investigative agency may be co-opted for political or personal gain.

Article 27 states that only an "authorised officer of the investigative agency shall have the powers to investigate an offence under this Act."[37] While this limitation on investigative authority is commendable, there are no requirements as to who may become an "authorised officer" or any criteria or procedure to name an "authorised officer." This issue becomes magnified since the "authorised officer" is empowered in Article 28[38] to preserve and acquire

[35] PECA, Article 1(3): "[PECA] shall apply to every citizen of Pakistan wherever he may be, and also to every other person for the time being in Pakistan."

[36] PECA, Article 26: "(1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act. (2) Unless otherwise provided for under this Act, the investigation agency and the authorised officer shall in all matters follow the procedure laid down in the Code to the extent that it is not inconsistent with any provision of this Act. (3) Notwithstanding provisions of any other law, the Federal Government shall make rules for appointment and promotion in the investigation agency including undertaking of specialized courses in digital forensics, information technology, computer science and other related matters for training of the officers and staff of the investigation agency."

[37] PECA, Article 27: "(1) Only an authorised officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams comprising of the authorised officer of investigation agency and any other law enforcement agency for investigation of offence under this Act and any other law for the time being in force."

[38] PECA, Article 28(1): "If an authorised officer is satisfied that- (a) data stored in any information system or by means of an information system, is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible, the authorised officer may, by written notice given to a person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not

any and all data "reasonably required for the purposes of a criminal investigation," if there is "a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible." The authorised officer only needs to be personally satisfied that such data is reasonably required for an investigation – there is no judicial oversight at this stage. The authorised officer is, however, required to inform a court within 24 hours that he/she has begun to acquire this data. The Court may then issue orders "deemed appropriate in the circumstances of the case," but Article 28 does not explicitly call for real judicial oversight because the Court is not explicitly given the power to overturn an authorised officer's order in the PECA. The judicial review required by Article 28 likely amounts to a *de facto* approval of law enforcement requests, which may lead or contribute to an impermissible restriction on the freedom of expression.[39]

Articles 30[40] and 31[41] outline the thresholds and standards needed for a warrant for search and seizure and a warrant for disclosure of data, respectively. Both articles explicitly state that once an authorised officer,[42] "demonstrates to the Court that there exist reasonable grounds to believe that the specified data…is reasonably required…" for an investigation or prosecution of a PECA offense, the Court may order such a warrant. The threshold to obtain warrants under Articles 30 and 31 is the very low, reasonable ground standard, which amounts to *de facto* approval.[43] Without higher threshold there is no real, meaningful judicial oversight. The PECA should be revised to require meaningful judicial oversight before issuing warrants for the search, seizure or disclosure of data.

---

exceeding ninety days as specified in the notice: Provided that the authorised officer shall immediately but not later than twenty four hours bring to the notice of the Court, the fact of acquisition of such data and the court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise."

[39] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 56, UN Doc. # A/HRC/23/40, (April 2013).

[40] PECA, Article 30: "Upon an application by an authorised officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that - (a) may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence made out under this Act; or (b) has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorise an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data or other articles relevant to the offence identified in the application."

[41] PECA, Article 31(1): "Upon an application by an authroised [sic] officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that specified data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that a person in control of the information system or data, to provide such data or access to such data to the authorised officer."

[42] It should again be noted that there are no requirements as to who can become an "authorised officer," no criteria for selecting these officers, and no requirements that the yet-to-established "investigative agency" delineate such requirements or criteria.

[43] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 56, UN Doc. # A/HRC/23/40, (April 2013).

Article 32 outlines the powers of an "authorised officer." While delineating these powers is important, Article 32 provides authorised officers with broad, sweeping powers but provides no judicial oversight.[44] Authorised officers can, amongst other powers, require any person that is in charge of, or concerned with, operations of any information system to provide reasonable technical assistance to him/her, require persons to decrypt devices or networks, and have unfettered access to, or demand, code and technology to unscramble or decrypt data. Forcing individuals or entities to turn over encryption keys or devices amounts to an impermissible restriction of freedom, and Pakistan should refrain from compelling the production of encryption keys.[45]

These authorised officer's powers are "constrained" in Article 32(2), stating, amongst other requirements, that he/she must act with "proportionality" and must avoid disruption to networks, businesses, or information systems.[46] Constraining the authorised officer's powers is commendable, however the constraints articulated in 32(2) are aspirational. There is no enforcement mechanism or judicial oversight.

---

[44] PECA, Article 32(1): "(1) Subject to provisions of this Act, an authorised officer shall have the powers to - (a) have access to and inspect the operation of any specified information system; (b) use or cause to be used any specified information system to search any specified data contained in or available to such system; (c) obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system; (d) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version; (e) require any person by whom or on whose behalf, the authorised officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person; (f) require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorised officer may require for investigation of an offence under this Act; and (g) require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence: Explanation.- Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data."

[45] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 89, UN Doc. # A/HRC/23/40, (April 2013).

[46] PECA, Article 32(2) and 32(3): "(2) In exercise of the power of search and seizure of any information system, program or data the authorised officer at all times shall- (a) act with proportionality; (b) take all precautions to maintain integrity of the information system and data in respect of which a warrant for search or seizure has been issued; (c) not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search or seizure has been issued; (d) avoid disruption to the continued legitimate business operations and the premises subjected to search or seizure under this Act; and (e) avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specified offence in respect of which a warrant has been issued. (3) When seizing or securing any information system or data, the authroised [sic] officer shall make all efforts to use technical measures while maintaining its integrity and chain of custody and shall only seize an information system, data, device or articles, in part or in whole, as a last resort, for sufficient reasons that do not make it possible under the circumstances to use such technical measures or where use of such technical measures by themselves would not be sufficient to maintain the integrity and chain of custody of the data being seized."

The broad powers given to authorised officers in Article 32, even with the constraints articulated in 32(2), are ripe for abuse because there is no meaningful judicial oversight, which will have a detrimental impact on the freedoms of expression and association and right to privacy. Article 32 should be revised to address these concerns.

Pursuant to Article 34, the Authority has broad powers to manage intelligence and remove or block access to intelligence.[47] The Authority or "any officer authorised by it"[48] can direct service providers to remove or block content. The criteria used by the Authority to justify the blocking or removal are extremely vague - "necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act." Vague, broad terms such as these may violate the requirements of the ICCPR.[49]

The term "any officer" is troubling as there are no requirements or criteria on how the Authority names an officer, and the PECA does not require the Authority to ever establish such criteria.[50] In order to safeguard fundamental freedoms, criteria to name the Authority's officers should be included in the PECA or the PECA should require the Authority to establish them in a certain, defined, reasonable amount of time.

Article 34(2) grants the Authority broad powers to establish rules of standards and procedures to "manage intelligence, block access and entertain complaints."[51] Article 34(3) permits the Authority to exercise its powers under the PECA "in accordance with the directions issued by the Federal Government" until such time as Authority develops its procedures and standards to manage intelligence.[52] However, there is no requirement that the Authority actually establish

[47] PECA, Article 34(1): " The Authority is empowered to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system. The Authority or any officer authorised by it in this behalf may direct any service provider, to remove any intelligence or block access to such intelligence, if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act."

[48] It is important to note that the officer described in Article 34 is a different officer from the "authorised officer" referred to in the PECA's other articles.

[49] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, para. 39, UN Doc. # A/66/290 (August 2011).

[50] It is important to note that the "officer" mentioned in Article 34 is different from the "officer" noted in Articles 27, 30, 31 and 32 and others: the former are officers of the Authority, the latter are officers of the investigatory agency referred to in Article 26.

[51] PECA, Article 34(2): "The Authority may prescribe rules for adoption of standards and procedure to manage intelligence, block access and entertain complaints."

[52] PECA, Article 34(3): "(3) Until such procedure and standards are prescribed, the Authority shall exercise its powers under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provisions of this Act."

such procedures and standards, and therefore the Authority is essentially given *carte blanche* to operate as it sees fit, restrained only by the orders of the Federal Government. There are no safeguards to protect the freedom of expression or right to privacy. Article 34 should be revised to place a firm time frame for the Authority to establish its procedures and standards and include legitimate safeguards to protect the freedom of expression and right to privacy.

Article 36 governs the real-time collection and recording of intelligence.[53] The initial period for real-time collection and recording is 7 days, but may be extended "for a further specified period,"[54] which could be indefinitely. This clause should be revised to limit the period of real-time collection and recording of intelligence, and should explicitly state periodic judicial reviews of such collection and recording orders.

Although the judicial threshold outlined in Article 36(1) to allow the real-time collection and recording of intelligence is low - that there exist "…reasonable grounds to believe that the specified data…is reasonably required…" for an investigation or prosecution of a PECA offense[55] – Article 36(5) provides a set of standards that must be included in any application for the real-time collection and recording of intelligence. Such application must: (1) state why the sought-after data is with a specific person; (2) identify and explain with specificity the type of intelligence likely to be found; (3) identify and explain with specificity the alleged offence; (4) state why more than one occasion is needed to capture the data and explain why; (5) explain the measures taken to ensure privacy of others; (6) explain why the investigation may be frustrated without real-time collection; and (7) explain why real-time collection is necessary to achieve the purpose of warrant.[56]

---

[53] PECA, Article 36(1): "If a Court is satisfied on the basis of information furnished by an authorised officer that there are reasonable grounds to believe that the content of any intelligence is reasonably required for the purposes of a specific criminal investigation, the Court may order, with respect to intelligence held by or passing through a service provider, to a designated agency as notified under the Investigation for Fair Trial Act, 2013 (I of 2013) or any other law for the time being in force having capability to collect real time intelligence, to collect or record such intelligence in real-time in coordination with the investigation agency for provision in the prescribed manner: Provided that such real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days."

[54] PECA, Article 36(3): "The period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorises an extension for a further specified period."

[55] The same concerns outlined above regarding this low judicial threshold are applicable here.

[56] PECA, Article 36(5): "The application under sub-sections (1) and (2) shall in addition to substantive grounds and reasons also- (a) explain why it is believed the data sought will be available with the person in control of an information system; (b) identify and explain with specificity the type of intelligence likely to be found on such information system; (c) identify and explain with specificity the identified offence made out under this Act in respect of which the warrant is sought; (d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why, and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued; (e) what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of intelligence of any person not part of the investigation; (f) why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) why to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

The required explanations for applications for the real-time collection and recording of intelligence are excellent safeguards to individuals' fundamental rights and freedoms. These explanations should be included in all warrants, collection orders, etc. under PECA.

The articles in Chapter III need to be revised so that the investigatory agency's powers and those of its officers are more clearly delineated and more narrowly tailored. Additional oversight and judicial review mechanisms should be inserted into Chapter III, with removal and blockage of content a last resort. Revising Chapter III in this manner will ensure a well-functioning investigatory agency and ensure compliance with international human rights standards.

ICNL remains available to provide technical assistance, as appropriate.

Respectfully submitted
May 8, 2015